FortiClient VPN (Android) v5.2.4
User Guide

FortiClient VPN (Android) v5.2.4 User Guide

October 9, 2014

04-524-234330-20141009

Fortinet Document Library	docs.fortinet.com
Fortinet Video Library	video.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2014-03-05	Initial release.
2014-07-09	Updated for FortiClient VPN (Android) v5.2.1.
2014-08-01	Updated for FortiClient VPN (Android) v5.2.2.
2014-08-20	Updated for FortiClient VPN (Android) v5.2.3.
2014-10-09	Updated for FortiClient VPN (Android) v5.2.4.

Introduction

FortiClient VPN (Android) v5.2 includes IPsec VPN, SSL VPN, and Endpoint Control.

FortiClient VPN (Android) v5.2 features

The following table lists and describes features supported in FortiClient VPN (Android) v5.2.

Table 1: FortiClient VPN (Android) features

Feature	Description
IPsec VPN	• Configure IPsec VPN connections. • Client X.509 certificates and pre-shared key support. • Enable always up and auto connect options. • Disable auto start.
SSL VPN	• Configure tunnel mode SSL VPN connections. • Client and server X.509 certificates support. • Enable always up and auto connect options. • Disable auto start.
Endpoint Control	• Configure and deploy a FortiOS FortiClient Profile to registered FortiClient VPN (Android) devices. • Provision VPN connections. • Policy enforcement.

Download FortiClient VPN (Android) v5.2.4

You can download the FortiClient VPN (Android) v5.2.4 application from the Google play application or at the following link, https://play.google.com/store.

Product Integration and Support

FortiClient VPN (Android) v5.2.4 support

The following table lists FortiClient VPN (Android) v5.2.4 product integration and support information.

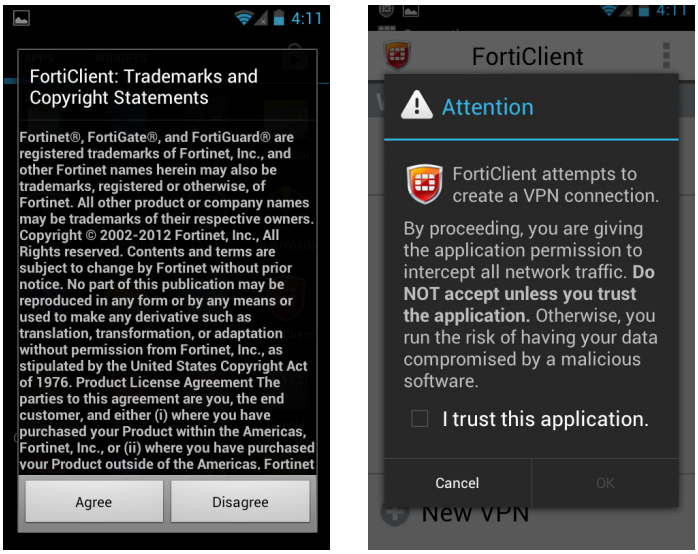
Table 2: FortiClient (Android) v5.2.4 support information

Android operating systems	• 4.0 Ice Cream Sandwich (API level 14, API level 15) • 4.1 Jelly Bean (API level 16) • 4.2 Jelly Bean (API level 17) • 4.3 Jelly Bean (API level 18) • 4.4.3 KitKat (API level 19) • 4.4.4 KitKat (API level 19)
FortiOS	• v5.0.5 and later • v5.2.0 and later
FortiToken Mobile	• v2.0.3 and later For more information, see the FortiToken Mobile 2.0 User Guide for Android.

Open the Application

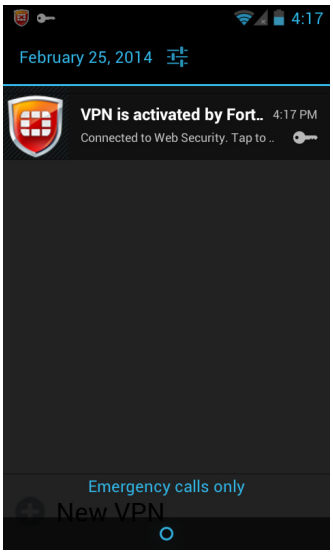
When FortiClient VPN (Android) v5.2 is installed and run for the first time, read the *Trademarks and Copyright Statement* and select the *Agree* button. Read the statement, select the *I trust this application* checkbox, and select *OK*. After that, FortiClient VPN (Android) will automatically start when Android OS starts.

Figure 1: Trademarks and VPN message



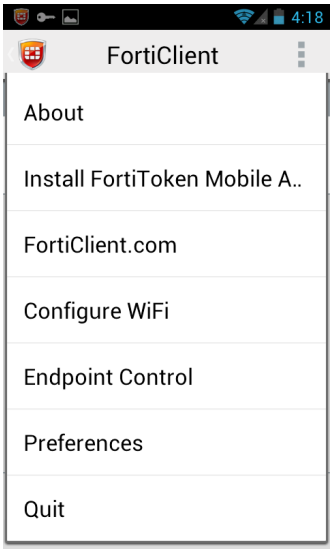
FortiClient VPN (Android) v5.2 allows you to launch the application from the notification bar.

Figure 2: Launch from notification bar



You can quit the app from the menu page.

Figure 3: Quit from app menu



SSL VPN

FortiClient VPN (Android) v5.2 supports tunnel mode SSL VPN connections. You can either configure the SSL VPN in the FortiClient user interface or provision SSL VPN connections in the FortiGate FortiClient Profile. Provisioned SSL VPN configurations are pushed to your Android device upon successful registration with the FortiGate device for Endpoint Control. You can configure X.509 certificates, CA server certificates, and check server certificates. You can also configure always up and auto connect for the VPN connection.

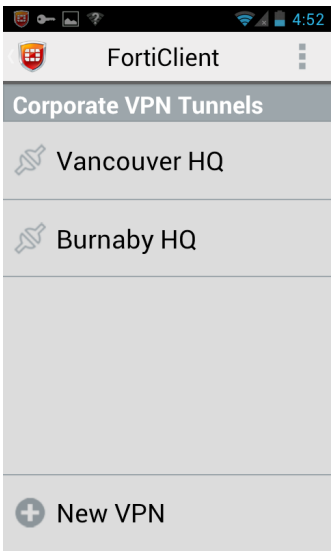
Create an SSL VPN connection

To create a new SSL VPN connection in the FortiClient VPN (Android) user interface follow the steps listed below.

To create a new SSL VPN connection:

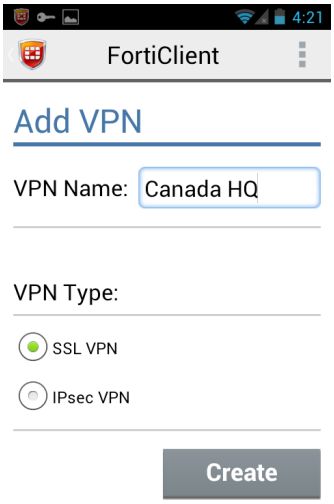
1. Select *New VPN* from the toolbar in the bottom of the page.

Figure 4: New VPN page



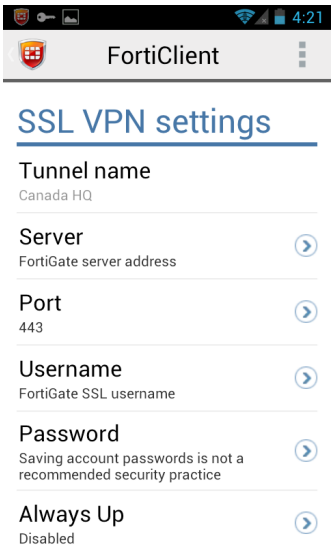
2. Enter a name for the new VPN connection, select *SSL VPN* under *VPN Type*, and select *Create*.

Figure 5: Add VPN settings page



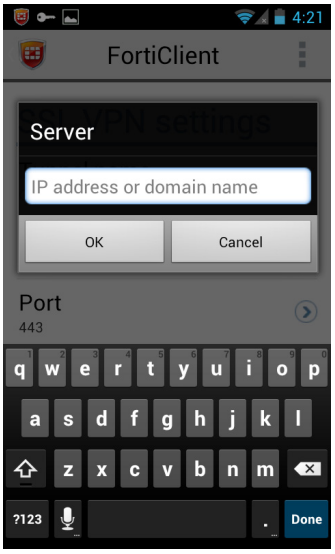
The SSL VPN settings page is displayed.

Figure 6: SSL VPN settings page



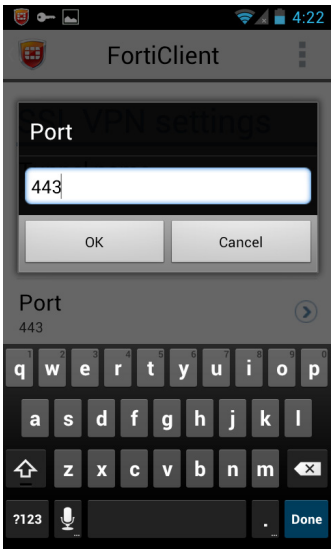
3. Select *Server,* enter the server IP address or domain name, and select *OK*.

Figure 7: Server dialog box



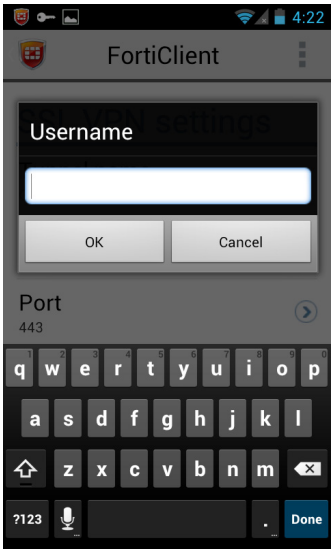
4. Select *Port*, enter the port number, and select *OK*. The default port is 443.

Figure 8: Port dialog box



5. Select *Username*, enter a user name, and select *OK*.

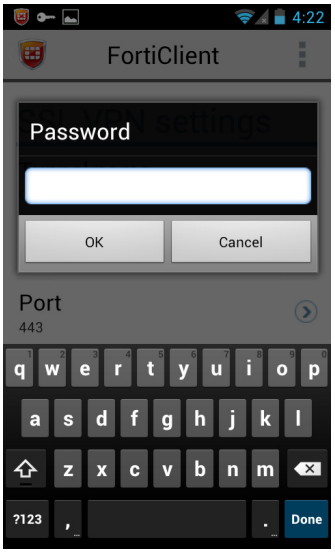
Figure 9: Username dialog box



6. Select *Password*, enter a password, and select *OK*. There is no maximum value for the password length. The password can consist of alpha, numeric and special characters.

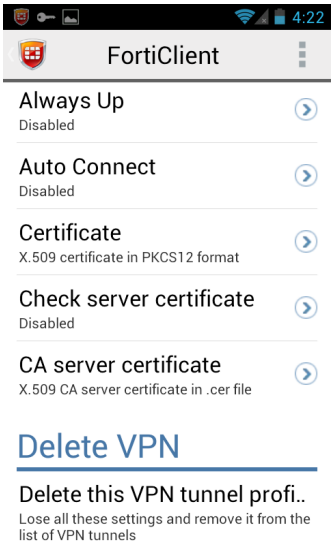
The username and password configured on the client must match the username and password configured on the FortiGate. Contact your network administrator for the correct setting.

Figure 10: Password dialog box



7. You can select to enable *Always Up*, *Auto Connect*, and *Check server certificate* in the *SSL VPN settings* page.

Figure 11: Optional settings



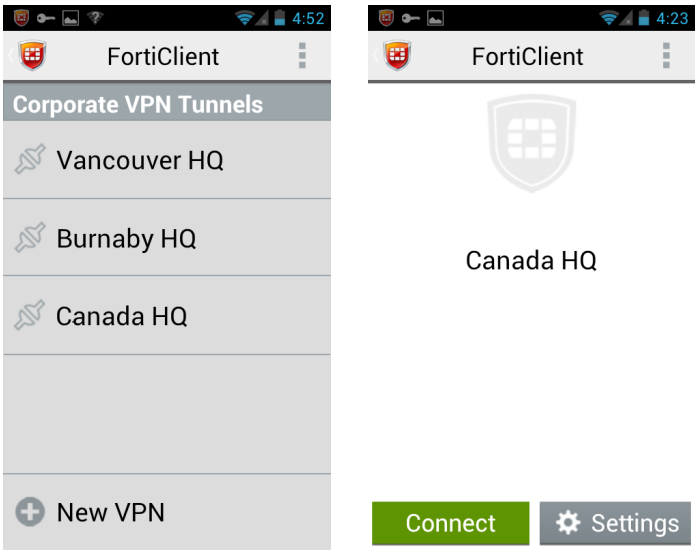
Connect to the VPN

SSL VPN tunnel mode uses X.509 Certificates (PKCS12 format) for authentication. Certificate settings need to be configured if authentication requires the client certificate, otherwise leave the certificate settings as their default value. For more information see “Client and Server CA Certificates” on page 16.

To connect to the SSL VPN:

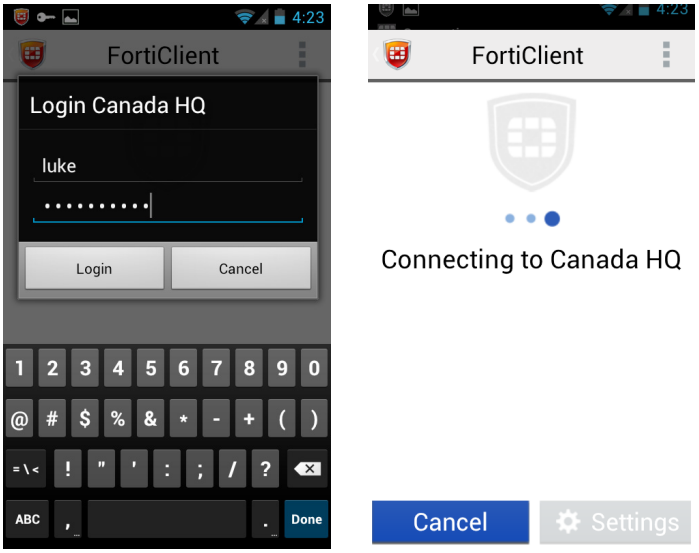
1. Select an available VPN and then select *Connect*.

Figure 12:VPN tunnels



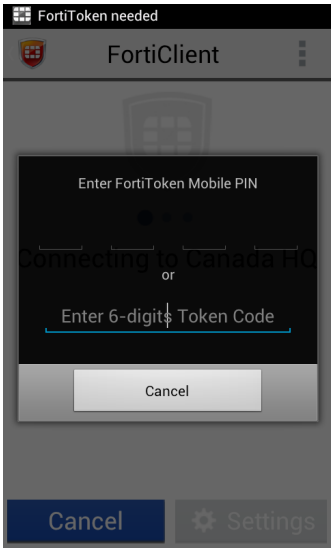
2. Enter your username and password and then select *Login*.

Figure 13: Login and connecting pages



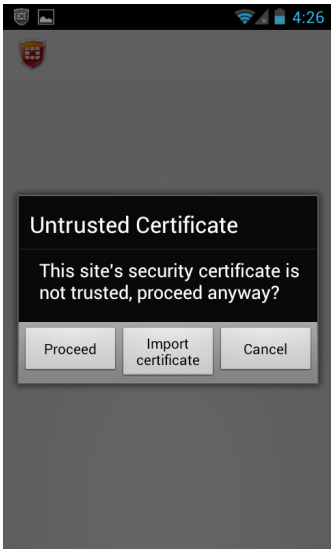
If the SSL VPN you are connecting to requires you to enter a FortiToken Mobile token, you will be prompted to enter your FortiToken Mobile PIN or 6-digit Token.

Figure 14: FortiToken Mobile page



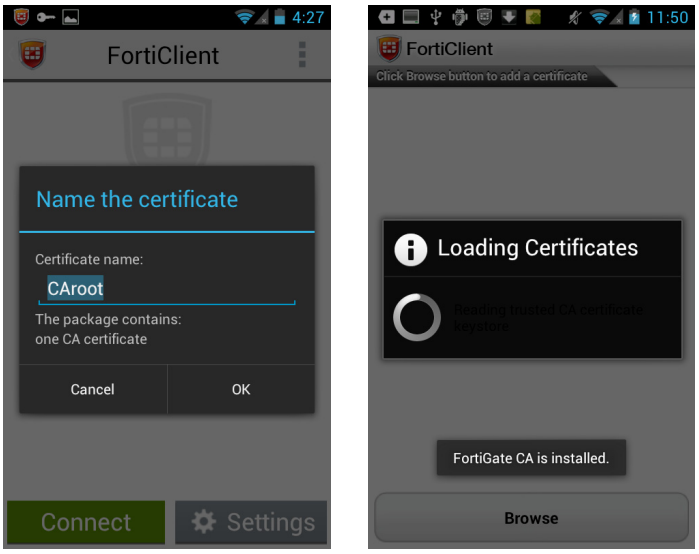
3. You will receive an *Untrusted Certificate* message dialog box warning message, and you will have the option to *Proceed*, *Cancel*, or *Import certificate*.

Figure 15: Untrusted Certificate dialog box



4. Select *Import certificate*, browse for the certificate file, edit the name (if required).

Figure 16: Certificate pages

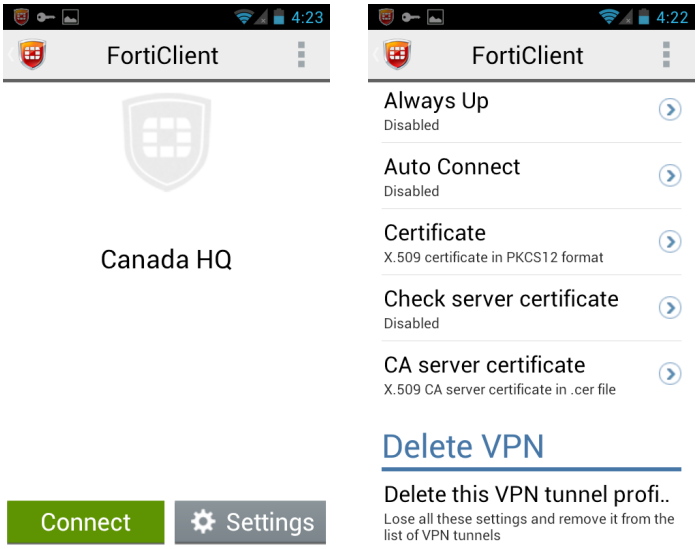


5. Select *OK* to load and install the certificate. The certificate is now installed on the device. Use the device back button to return to the connection screen.
6. Select an available VPN to connect.

Edit SSL VPN settings or delete a SSL VPN configuration

To edit SSL VPN settings or delete an existing SSL VPN configuration, select the SSL VPN, and select the *Settings* button.

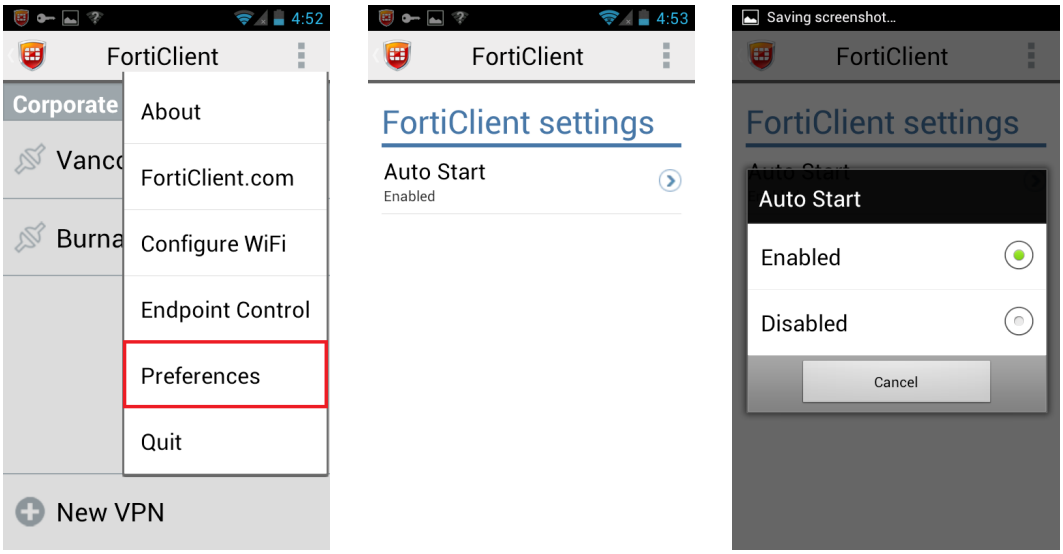
Figure 17:VPN settings pages



Auto start

In FortiClient VPN (Android) v5.2 you can select to disable auto start. To enable or disable auto start, select the menu icon in the toolbar, and select *Preferences* in the drop-down menu. In the FortiClient settings page select *Auto Start* and select *Enabled* or *Disabled*.

Figure 18: Auto start option



IPsec VPN

FortiClient VPN (Android) v5.2 supports IPsec VPN connections. You can either configure the IPsec VPN in the FortiClient user interface or provision IPsec VPN connections in the FortiGate FortiClient Profile. Provisioned IPsec VPN configurations are pushed to your Android device upon successful registration with the FortiGate device for Endpoint Control. You can configure server settings, phase 1, phase 2, and XAuth settings.

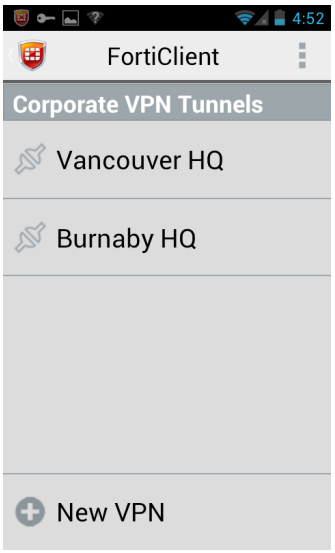
Create an IPsec VPN connection

To create a new IPsec VPN connection in the FortiClient VPN (Android) user interface follow the steps listed below.

Create a new IPsec VPN connection:

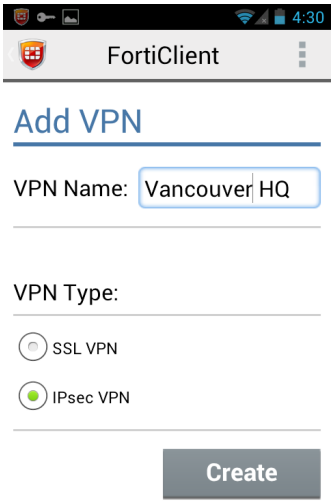
1. Select *New VPN* from the toolbar in the bottom of the page.

Figure 19: New VPN page



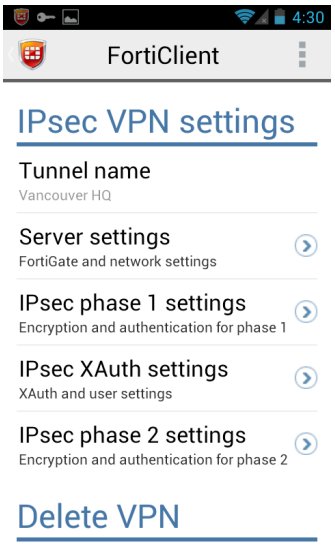
2. Enter a name for the new VPN connection, select *IPsec VPN* under *VPN Type*, and select *Create*.

Figure 20: Add VPN page



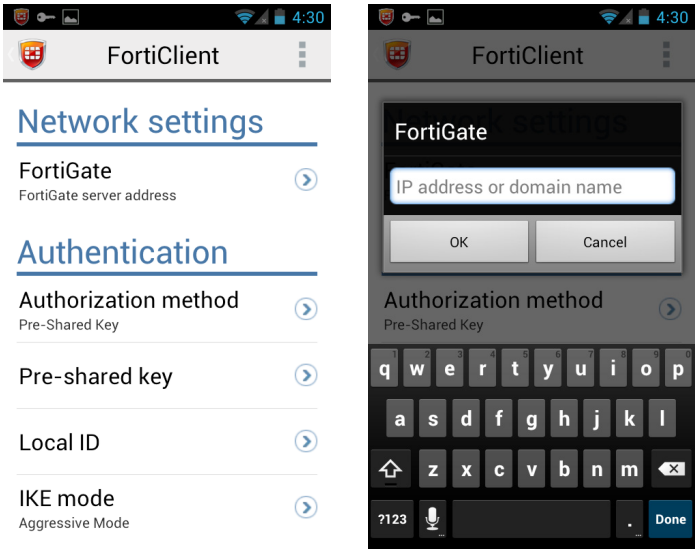
The IPsec VPN settings page is displayed.

Figure 21:IPsec VPN settings page



3. Select *Server settings*, under *Network settings*, select *FortiGate*, enter the server IP address or domain name, and select *OK*.

Figure 22: Network settings and FortiGate pages



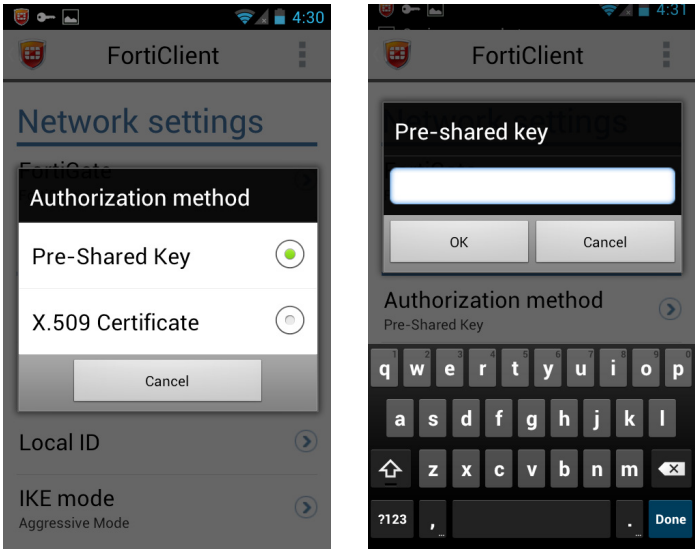
4. Under *Authentication*, select *Authorization method*, and select either *Pre-Shared Key* or *X.509 Certificate*.
5. For pre-shared key, select *Pre-shared Key* to enter the pre-shared key value.

   The simplest way to authenticate with the FortiGate unit is by means of a pre-shared key. This is less secure than using certificates, especially if it is used alone, without requiring peer IDs or extended authentication (XAuth).

   The pre-shared key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters.

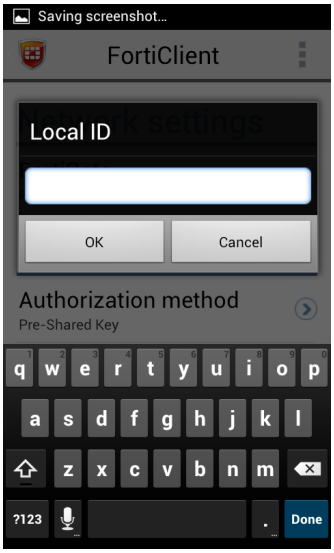
The pre-shared key configured on the client must match the pre-shared configured on the FortiGate. Contact your network administrator for the correct setting.

Figure 23: Authorization method and pre-shared key pages



a. Select *Local ID*, enter the local ID, and select *OK*.

Figure 24: Local ID page



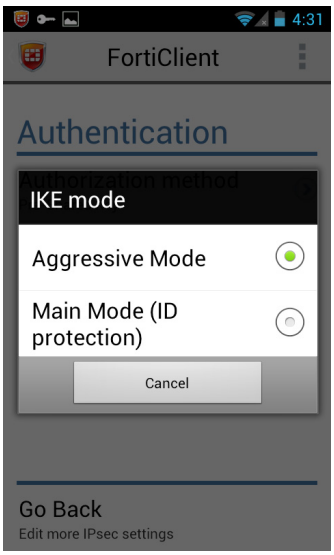
6. For X.509 certificate select *Certificate* and then browse for the certificate file on your device.

   To authenticate with the FortiGate unit using digital certificates, you must have the required certificates installed on the Android device (peer) and the FortiGate unit (server).

Contact your network administrator for the correct X.509 certificate file.

7. Select *IKE mode*, and select *Aggressive Mode* or *Main Mode (ID protection)*.

Figure 25:IKE mode page



In *Aggressive Mode*, the phase 1 parameters are exchanged in single message with authentication information that is not encrypted.

In *Main Mode*, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information.

The *IKE Mode* selected on the client must match the mode selected on the server. Contact your network administrator for the correct setting.

8. Select *Go Back* to return to the *IPsec VPN settings* page.
9. Select *IPsec phase 1 settings* to view or edit the phase 1 proposal encryption and authentication settings. You can choose to use the default settings.

   Select the encryption and authentication algorithms that will be used to generate keys for protecting negotiations. You can select any of the following symmetric-key algorithms:

   - DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
   - 3DES: Triple-DES, in which plain text is encrypted three times by three keys.
   - AES128: A 128-bit block algorithm that uses a 128-bit key.

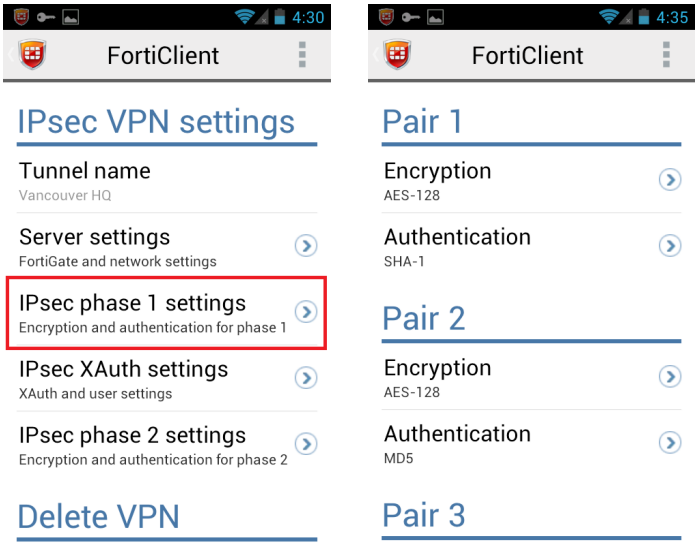
   You can select one of the following message digests to check the authenticity of messages during phase 1 negotiations:

   - MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.
   - SHA-1: Secure Hash Algorithm 1, which produces a 160-bit message digest.

   Select one or more Diffie-Hellman (DH) groups from DH group 1, 2, 5, and 14. When using aggressive mode, DH groups cannot be negotiated.

Contact your network administrator for the correct phase 1 encryption and authentication algorithms, and DH group.

Figure 26: Phase 1 settings pages



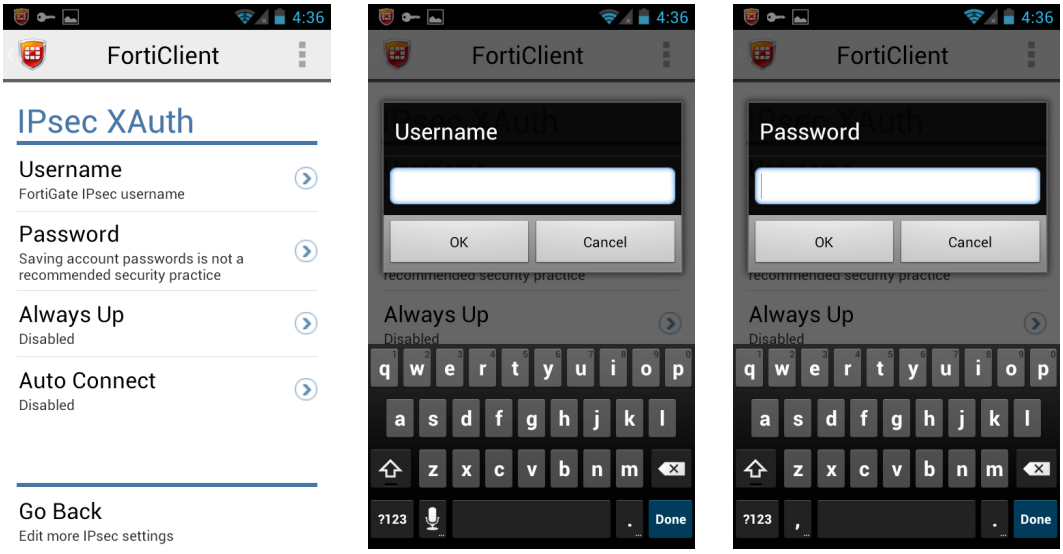
10. Select *Go Back* to return to the *IPsec VPN settings* page.

11. Select *IPsec XAuth settings* to view or edit the XAuth and user settings. XAuth is enabled by default. Select *Username* to enter the FortiGate IPsec username. Select *Password* to enter the password value. To use XAuth, you must first configure the user's credentials on your FortiGate, and external RADIUS or LDAP server.

    Extended authentication (XAuth) increases security by requiring the remote dialup client user to authenticate in a separate exchange at the end of phase 1. XAuth draws on existing FortiGate user group definitions and uses established authentication mechanisms such as PAP, CHAP, RADIUS and LDAP to authenticate dialup clients.

    You can select to enable *Always Up*, *Auto Connect*, and *Check server certificate* in the *IPsec XAuth* page.

Figure 27: XAuth username and password pages



12. Select *Go Back* to return to the *IPsec VPN settings* page.
13. Select *IPsec phase 2 settings* to view or edit the phase 2 encryption and authentication settings. You can choose to use the default settings.

    Select the encryption and authentication algorithms that will be used to generate keys for protecting negotiations. You can select any of the following symmetric-key algorithms:

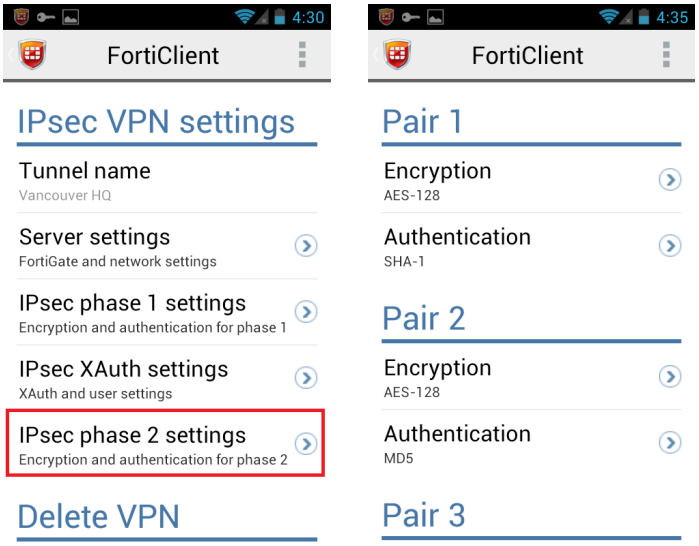
    - DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
    - 3DES: Triple-DES, in which plain text is encrypted three times by three keys.
    - AES128: A 128-bit block algorithm that uses a 128-bit key.

    You can select one of the following message digests to check the authenticity of messages during phase 1 negotiations:

    - MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.
    - SHA-1: Secure Hash Algorithm 1, which produces a 160-bit message digest.

    Select one or more Diffie-Hellman groups from DH group 1, 2, 5, and 14. When using aggressive mode, DH groups cannot be negotiated.

Figure 28: Phase 2 settings pages



Contact your network administrator for the correct phase 2 encryption and authentication algorithms, and DH group.

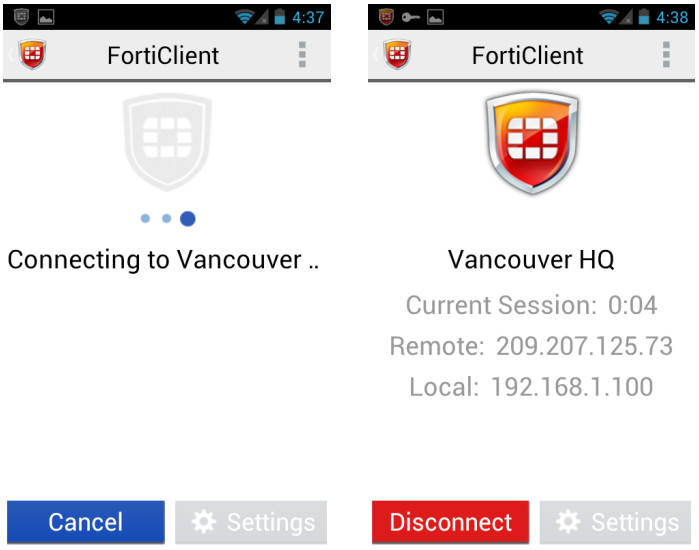
14. Select *Go Back* to return to the *IPsec VPN settings* page.

Connect to an IPsec VPN

Connect to an IPsec VPN:

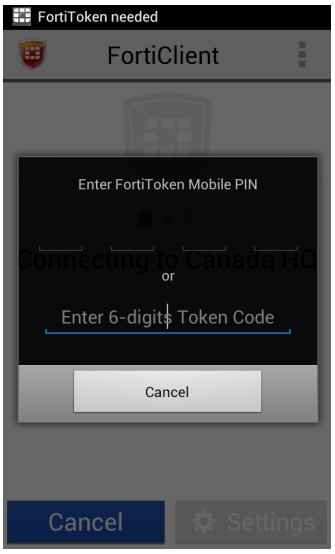
1. Select an available IPsec VPN connection.
2. Enter the username and password, and select *Connect*.

Figure 29:IPsec connection page



If the IPsec VPN you are connecting to requires you to enter a FortiToken Mobile token, you will be prompted to enter your FortiToken Mobile PIN or 6-digit Token.

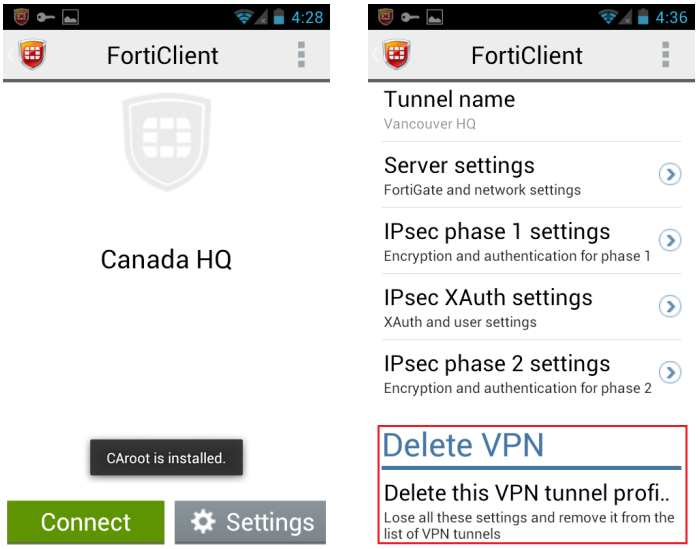
Figure 30: FortiToken Mobile page



Edit VPN settings or delete a VPN configuration

To edit IPsec VPN settings or delete an existing IPsec VPN configuration, select the IPsec VPN, and select the *Settings* button.

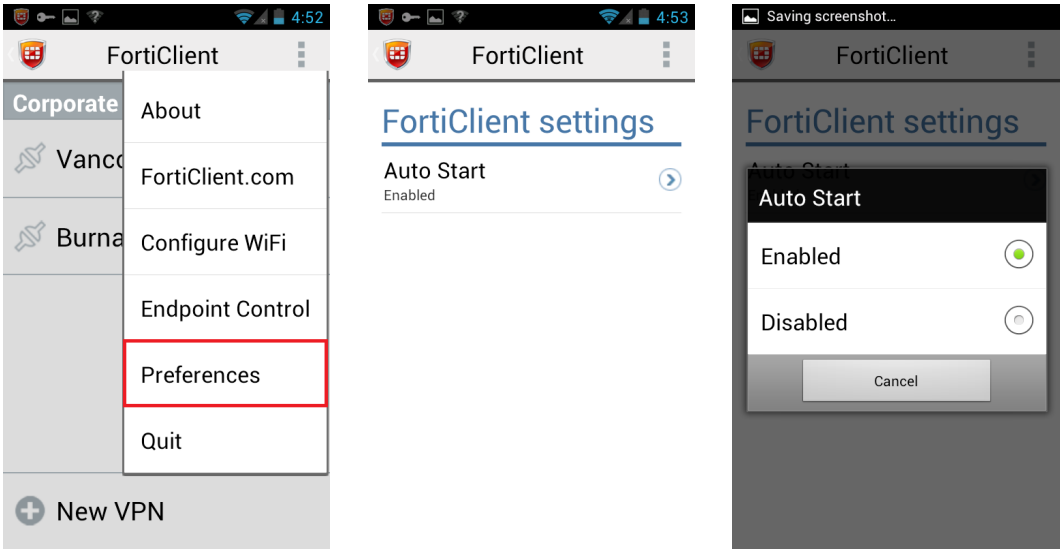
Figure 31:VPN settings pages



Auto start

In FortiClient VPN (Android) v5.2 you can select to disable auto start. To enable or disable auto start, select the menu icon in the toolbar, and select *Preferences* in the drop-down menu. In the FortiClient settings page select *Auto Start* and select *Enabled* or *Disabled*.

Figure 32: Auto start option



Endpoint Control

FortiClient VPN (Android) v5.2 allows you to register to a FortiGate device and receive a FortiClient Profile for endpoint control. For more information on configuring endpoint management, see the *FortiClient Administration Guide* and *FortiOS Handbook* available in the Fortinet Document Library.

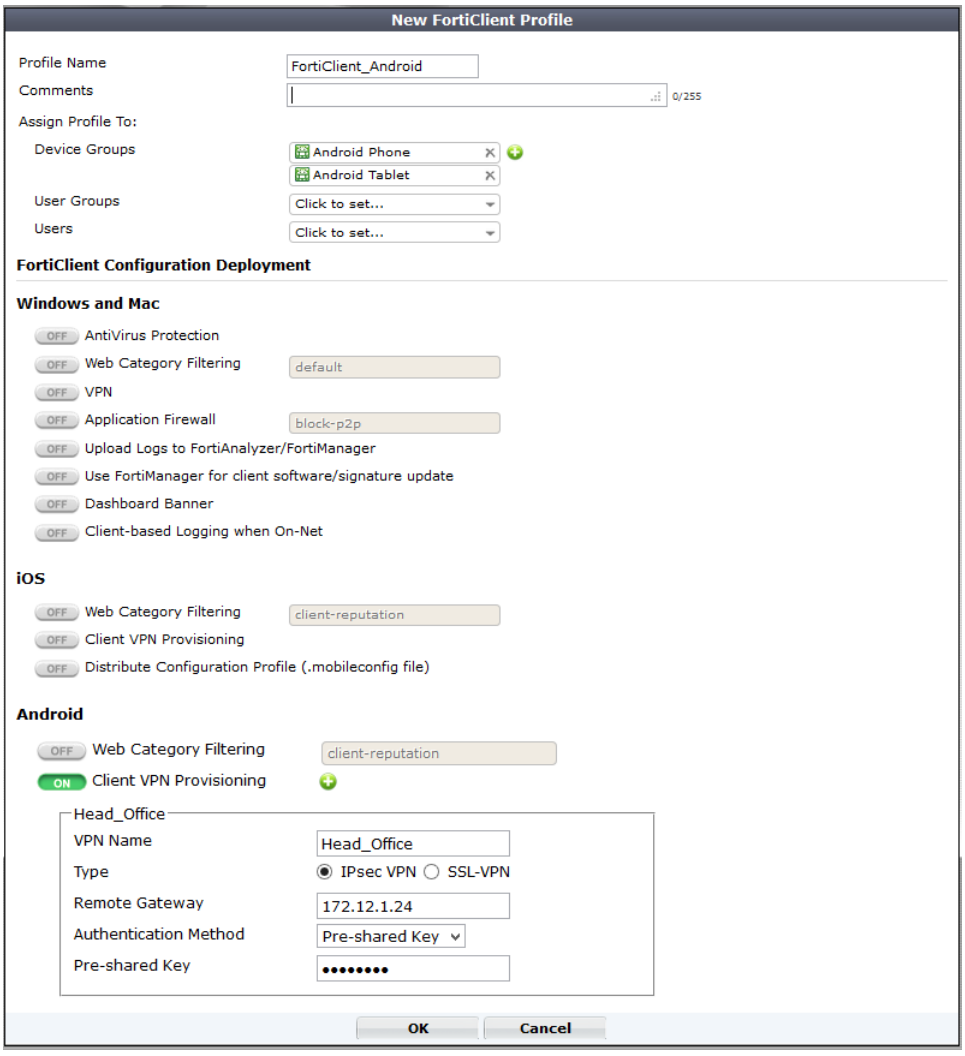
FortiGate FortiClient Profile

Configure the FortiClient Profile:

1. On your FortiGate device, go to *User & Device* > *FortiClient Profiles*.
2. Select *Create New* from the toolbar.

   The *New FortiClient Profile* page opens.

Figure 33: New FortiClient Profile page



3. In the *Android* section of the page, configure the following settings:

Client VPN Provisioning	Toggle the button to enable or disable client VPN provisioning. Select the add icon, , to add multiple VPN configurations.
VPN Name	Enter a name for the VPN connection.
Type	Select either IPsec VPN or SSL VPN.
Remote Gateway	Enter the remote gateway.
Authentication Method	Configure authentication settings. The options available are dependent on the type of VPN selected.

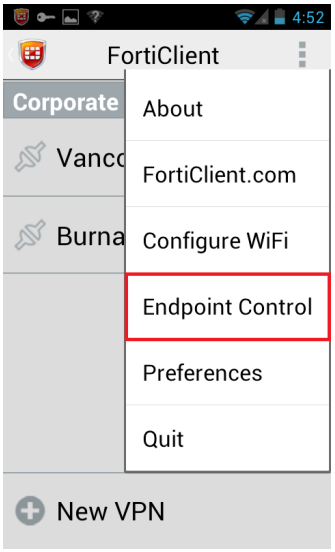
4. Select *OK* to save the settings.

Register to FortiGate

Register to the FortiGate:

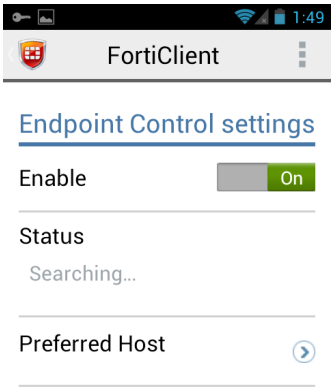
1. On your Android device, open the FortiClient VPN (Android) application.
2. Select the menu icon in the toolbar and select *Endpoint Control*.

Figure 34: Select Endpoint Control in menu



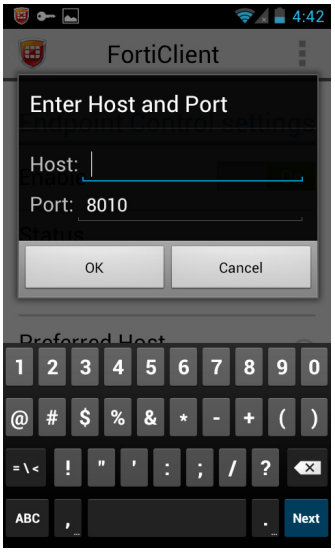
3. In *Endpoint Control settings* toggle the *Enable* switch to *On*.

Figure 35: Enable Endpoint Control



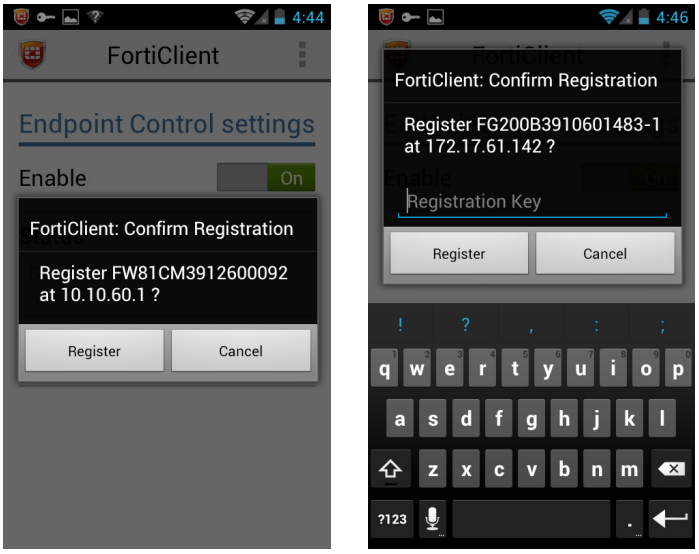
4. FortiClient VPN (Android) will search for available FortiGate devices. Alternatively, you can select *Preferred Host* and enter the FortiGate host IP and port number.

Figure 36: Preferred host page



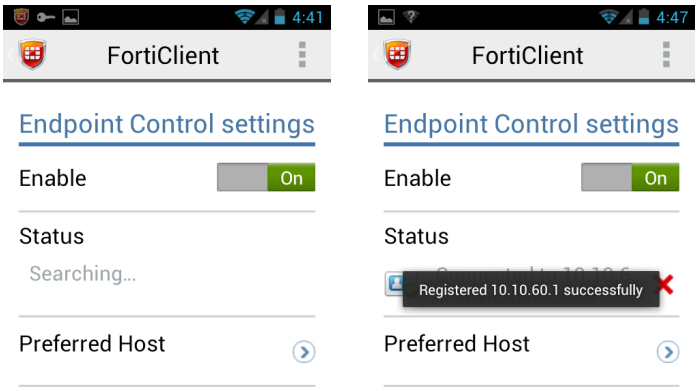
5. When a FortiGate is discovered you will receive a confirm registration dialog box with the FortiGate serial number and IP address. Depending on the FortiGate configuration, you may be required to enter a FortiClient registration key.

Figure 37: Confirm registration dialog box variations



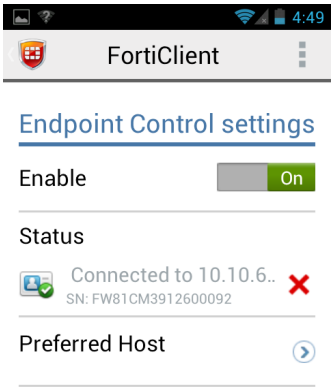
6. Select the *Register* button to continue. You will receive a confirmation dialog box when registration is complete.

Figure 38: Searching and registration complete



7. The *Endpoint Control settings* page will display a connected status.

Figure 39: Connected status



8. Upon successful registration with FortiGate, FortiClient VPN (Android) will receive the FortiClient Profile.

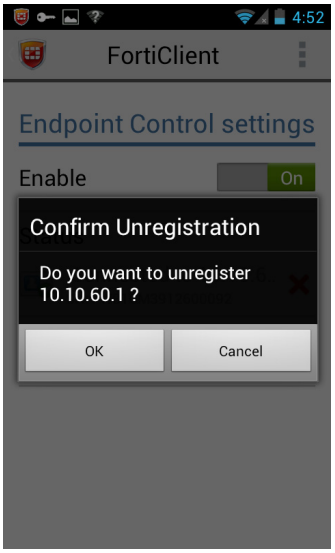
If FortiClient VPN (Android) is registered to FortiGate, it will auto start when the phone is turned on and bring up the GUI.

Unregister from FortiGate

To unregister from FortiGate:

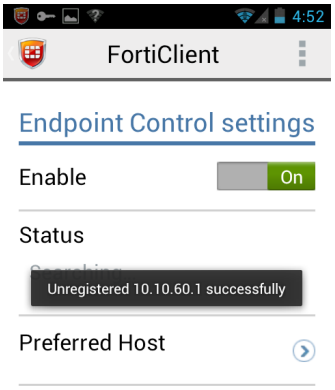
1. To unregister from FortiGate, in *Endpoint Control* settings page, in the *Status* section, select the red 'X' icon.
2. You will receive a confirmation dialog box.

Figure 40: Confirmation dialog box



3. Select *OK* to unregister from the FortiGate. You receive a confirmation dialog box advising that you are unregistered from the FortiGate.

Figure 41: Unregistered from FortiGate



4. Toggle the *Endpoint Control Enable* switch to *Off*.